UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff v. ANTHONY PELAYO, Defendant.	CASE NO. CR18-217RSM ORDER DENYING DEFENDANT PELAYO'S MOTION TO SUPPRESS EVIDENCE FROM ICLOUD ACCOUNT

This matter comes before the Court on Defendant Pelayo's Motion to suppress evidence obtained from his iCloud Account. Dkt. #444. The Government has filed an opposition brief. Dkt. #532. The Court finds it can rule without oral argument or an evidentiary hearing.

The Court will not recount the lengthy background of this case, adequately set forth by the Government, *see* Dkt. #532. At this late stage the background is well known to the parties.

Mr. Pelayo's Motion can be divided into two sections. First, he points to his joinder in a codefendant's Motion to Suppress and argues "[i]n the absence of evidence obtained in the search and seizure at issue in Docket number 65 there is no probable cause in the warrant application affidavit to justify the seizure of Mr. Pelayo's Apple iCloud account." Dkt. #444 at 3. The Government responds that even if this evidence was obtained via illegal searches of Mr. Woolard's property (the subject of the Motion at Dkt. #65), it would still be admissible as to

Pelayo "because Pelayo has no reasonable expectation of privacy in Woolard's property" and thus "any alleged illegality of the search of *Woolard's* properties does not violate *Pelayo's* Fourth Amendment rights." Dkt. #532 at 15 (citing *Wong Sun v. United States*, 371 U.S. 471, 492 (1963)) (emphasis in original).

The parties first briefed this issue with Mr. Pelayo's notice of joinder (Dkt. #365) to Mr. Woolard's Motion (Dkt. #65), and the Government's Response (Dkt. #374). Mr. Pelayo's position was that "[t]he fruits of the illegal search conducted against Mr. Woolard were used as the basis for searches of Mr. Pelayo's cell phone data and text messages," and that, although there is a rule that "a defendant may only challenge a search if he had a personal expectation of privacy in the target of the search," Mr. Pelayo "had a reasonable expectation of privacy in the electronic data stored in his iCloud account as well as other personal data revealed by subsequent searches in this case." Dkt. #365 at 1–2. The Government's response makes clear that the searches at issue were conducted at Mr. Woolard's properties (not Mr. Pelayo's), where Mr. Pelayo never lived or stayed as a guest, and that there is no evidence that seized property was owned by Mr. Pelayo. Dkt. #374. The Government argues, "'[e]vidence that has been suppressed against one defendant may be used against another defendant whose rights were not violated by the illegal search.'" *Id.* at 6 (citing Wright & Miller, 3A Fed. Prac. & Proc. Crim. § 687 (4th ed.)).

To claim Fourth Amendment protection, a defendant must demonstrate that he personally has an expectation of privacy in the place searched, and that his expectation is reasonable. *Rakas v. Illinois*, 439 U.S. 128, 143 (1978) ("...capacity to claim the protection of the Fourth Amendment depends... upon whether the person who claims the protection of the Amendment has a legitimate expectation of privacy in the invaded place."). The burden of proof is on the

defendant to show he has a reasonable expectation of privacy. *United States v. Caymen*, 404 F. 3d 1196, 1199 (9th Cir. 2005).

Mr. Pelayo has failed to demonstrate that he had a personal expectation of privacy in the target of the searches at issue in Dkt. #65—Mr. Woolard's residences. He does not have a basis to challenge those searches under the Fourth Amendment. *See Rakas, supra*. Even defendants charged as coconspirators must show independent, personal, reasonable expectations of privacy to maintain a Fourth Amendment challenge. *See United States v. Padilla*, 508 U.S. 77, 82 (1993); *see also United States v. Padilla*, 111 F.3d 685, 687 (9th Cir. 1997) ("Mere membership or participation in a conspiracy does not establish standing for purposes of the Fourth Amendment."). Mr. Pelayo's expectation of privacy as to the electronic data stored in his iCloud account is weighed against the different grounds for *that* search, conducted later and somewhere else. Mr. Pelayo may not join in Mr. Woolard's Motion, this cannot serve as a basis to question the probable cause for the later warrant as to his iCloud account, and this first argument fails.

The rest of Mr. Pelayo's Motion argues that the warrant to search his iCloud account was based on stale information and was "an unconstitutional general warrant with lack of particularity, overbreadth, and without temporal limitations as to search or retention of seized evidence." Dkt. #444 at 3. The warrant at issue authorized the seizure of all information from Apple related to Mr. Pelayo's iCloud account, including a wide variety of examples of what was to be seized. *See* Dkt. #444-1 at 5–9. Mr. Pelayo does not go through all of these items in detail, but focuses on examples that he deems overbroad. He relies heavily on *United States v. Wey*, 256 F. Supp. 3d 355, 379, (SD NY 2017) in his discussion of overbreadth and the retention of seized evidence.

The Government responds that it followed a standard two-step process for warrants under Rule 41(e)(2)(B) and the Electronic Communications Privacy Act, and that it would not have been feasible for the warrant to impose temporal or content restrictions on the initial seizure. *See* Dkt. #532 at 17–18. Such arguments were made by the Government in response to a similar Motion by Mr. Woolard. *See* Dkt. #531 at 2. In both that brief and this one, the Government cites an email from Apple indicating that certain files being turned over contained "aggregated data where Apple was unable to apply a date filter," and where Apple advised that "you may need to work with a cellular forensics expert to access and review the provided data." Dkt. #531-1 at 1. The Government goes on to cite *United States v. Sam*, 2020 WL 2131285, CR19-0115-JCC (WDWA May 5, 2020) as a recent case that addressed this issue. The Government favorably contrasts what was done with Mr. Pelayo's data with *Wey*, *supra*, and argues that this search warrant was executed in a reasonable manner. Dkt. #532 at 30.

"The Fourth Amendment was designed to prevent law enforcement officers from engaging in 'general exploratory searches.'" *United States v. Shi*, 525 F.3d 709, 731 (9th Cir. 2008). To achieve that goal, the Fourth Amendment imposes several requirements on a search warrant, one being that a warrant must not be overbroad. *Shi*, 525 F.3d at 731–32. In analyzing whether a warrant is overbroad, the Ninth Circuit considers three factors: (1) whether probable cause exists for seizure of all items described in the warrant; (2) if there are objective standards in the warrant that allow officers to distinguish between items subject to seizure from items not subject to seizure; and (3) whether the items described in the warrant could be described with more particularity considering the information available. *Shi*, 525 F.3d at 731–32.

Other than as addressed above, Mr. Pelayo does not contest that the Government had probable cause for seizure. With respect to the second *Shi* factor, the Court finds that this warrant

had objective standards to guide the search of Mr. Pelayo's iCloud account, which were set forth in Part II of Attachment B. The Court finds that the warrant had sufficient particularity under the circumstances. The Court finds that, like in *Sam*, *supra*, the warrant issued here was not required to include a temporal restriction on the seizure of the account because the entire account needed to be searched to find "records pertaining to the alleged crimes that occurred between January 1, 2013, and the present" and to link the account to Mr. Pelayo. The nature of the way the information was stored made it impractical for Apple to apply temporal or content restrictions. The Court agrees with *Sam* as to there not being a constitutional requirement for the Government to use a filter team in this case. *See* 2020 WL 2131285 at *3. The Court further finds that, unlike in *Wey, supra*, this search warrant was executed in a reasonable manner.

Mr. Pelayo argues that the search warrant affidavit relied on text messages "sufficiently remote in time as to not provide a reasonable likelihood evidence of continuing criminal activity will be found upon seizure of Mr. Pelayo's iCloud account." Dkt. #444 at 18–19.

The Ninth Circuit has explained that "[i]nformation underlying a warrant is not stale 'if there is sufficient basis to believe, based on a continuing pattern or other good reasons, that the items to be seized are still on the premises.'" *United States v. Schesso*, 730 F.3d 1040, 1047 (9th Cir. 2013) (citations omitted).

The Court agrees with the Government that there was a sufficient basis to believe, based on the pattern established by the submitted evidence and the expert opinion of Special Agent Cheng, that the items to be seized were still in the iCloud account to be searched.

Given all of the above, the Court finds Mr. Pelayo has failed to demonstrate any valid basis to suppress this evidence. Having reviewed the briefing, along with the remainder of the

record, the Court hereby finds and ORDERS that the Defendant Pelayo's Motion to Suppress Evidence from iCloud Account, Dkt. #444, is DENIED.

DATED this 4th day of June, 2021.

RICARDO S. MARTINEZ
CHIEF UNITED STATES DISTRICT JUDGE